



# **NIST Industrial Control System Security Activities**

**Keith Stouffer**

**National Institute of Standards and Technology**

**Information Security and Privacy Advisory Board (ISPAB) Meeting**

**Doubletree Hotel, Rockville, MD**

**June 9, 2005**

**NIST**

**National Institute of Standards and Technology**  
Technology Administration, U.S. Department of Commerce

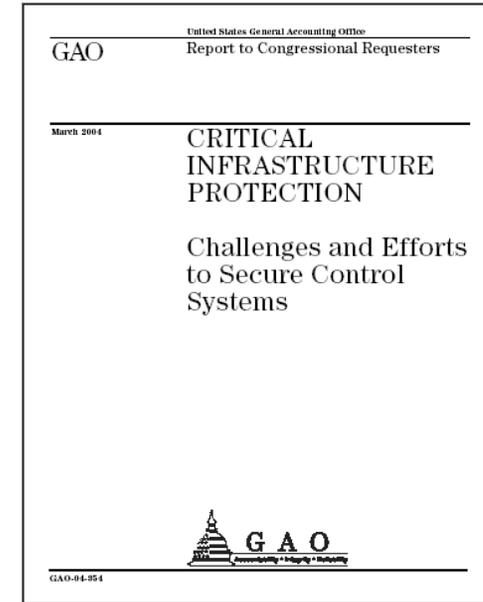


Intelligent Systems Division  
Manufacturing Engineering Laboratory



# Industrial Control System Security

- The (US) National Plan for Information Systems Protection and the recently released GAO-04-354 cite industrial control systems as critical points of vulnerability in America's utilities and industrial infrastructure...  
*“...Successful attacks on control systems could have devastating consequences, such as endangering public health and safety.”*



Electric power — Water — Oil & Gas  
Chemicals — Pharmaceuticals  
Mining, Minerals & Metals  
Pulp & Paper — Food & Beverage  
Consumer Products  
Discrete Manufacturing  
(automotive, aerospace,  
durable goods)





# Information Technology vs. Industrial Control Systems

## Different Performance Requirements

<b>Information Technology</b>	<b>Industrial Control</b>
Non-Realtime	Realtime
Response must be reliable	Response is time critical
High throughput demanded	Modest throughput acceptable
High delay and jitter accepted	High delay and/or jitter is a serious concern



# Information Technology vs. Industrial Control Systems

---

## Different Reliability Requirements

<b>Information Technology</b>	<b>Industrial Control</b>
Scheduled operation	Continuous operation
Occasional failures tolerated	Outages intolerable
Beta testing in the field acceptable	Thorough testing expected



# Information Technology vs. Industrial Control Systems

## Different Risk Management Requirements Delivery vs. Safety

<b>Information Technology</b>	<b>Industrial Control</b>
Data integrity paramount	Human safety paramount
Risk impact is loss of data, loss of business operations	Risk Impact is loss of life, equipment or product
Recover by reboot	Fault tolerance essential

These differences create huge differences in acceptable security practice



# Information Technology vs. Industrial Control Systems

## Different Security Architectures

<b>Information Technology</b>	<b>Industrial Control</b>
<p>The central server is the critical device for protection (not the edge client)</p>	<p>The edge device, such as the PLC or smart drive controller, is considered more important than a central host such as a data historian server</p>



# Industrial Control System (ICS) Security Challenges

---

- Real time constraints - IT security technology can impact timing, inhibit performance (response times are on the order of ms to s)
- Balancing of performance, reliability, flexibility, safety, security requirements
- Difficulty of specifying requirements and testing capabilities of complex systems in operational environments
- Security expertise and domain expertise required, but are often separated



# ICS Security Program Summary

---

- **Goal:** To develop standards and test methods to enable the integration of security engineering into the industrial automation life cycle, including design, implementation, configuration, maintenance and decommissioning. This goal supports the objectives of the NIST Homeland Security Strategic Focus Area
- **Outcome:** Reduced likelihood of successful cyberattack on the nation's critical infrastructure
- **NIST Role:** Working with industry to develop standards and test methods for validation and conformance



# NIST ICS Security Activities

Approximately 3 FTE Level of Effort

---

- Process Control Security Requirements Forum (PCSRF)
- System Protection Profile for Industrial Control Systems (SPP-ICS)
- SCADA Protection Profile
- SP800 Guide for SCADA and ICS Security
- ICS Vendor Security Checklist Program
- Industrial Control System Security Testbed
- Support related efforts (ISA SP-99, DHS Process Control Systems Forum (PCSF), I3P SCADA Initiative, AGA 12 SCADA Cryptography, IEC/ISO 65C, etc.)



# Process Control Security Requirements Forum (PCSRF)

Securing future systems:

Public/private partnership started in spring 2001 to increase the security of industrial process control systems through the definition and application of a common set of information security requirements for these systems.

Based on the *ISO 15408*  
*Common Criteria for IT Security*  
*Evaluation*





# Collaborators/Partners

Approximately 650 registered members including:

## ICS Vendors



## Government



## IT Vendors



## Standards Organizations



ISA-SP99



ISO/IEC 15408,  
19791, 61508, 65C



AGA 12

## End Users



Georgia-Pacific



ChevronTexaco

ExxonMobil



# PCSRF Membership

---

On 5/31/05 There were:

- 648 individual members from
- 215 organizations from
- 27 Countries (USA, Canada, Australia, Austria, Chile, China, France, Germany, Hong Kong, India, Ireland, Israel, Italy, Japan, Netherlands, New Zealand, Norway, Panama, Portugal, Russia, Saudi Arabia, Singapore, South Africa, Sweden, Switzerland, UK, Venezuela)



# PCSRF Website

<http://www.isd.mel.nist.gov/projects/processcontrol>

Google search for “industrial control security” or “process control security” returns the PCSRF site as the first (most valid) listing

SPP-ICS downloaded over 20,000 times

Website had nearly 100,000 server requests

Manufacturing Engineering Laboratory  
ISD's Research Areas  
NIST  
National Institute of Standards and Technology

ISD Home About ISD Research Areas Products and Services What's New Search

## Process Control Security Requirements Forum (PCSRF)



### Welcome

This site is a resource for users, vendors, and third parties in the process control industry who are concerned about information security in an increasingly networked world.

Through the NIST initiative on **Critical Infrastructure Protection (CIP)**, we are supporting the development and dissemination of standards for process control security. We have established the Process Control Security Requirements Forum (PCSRF), a working group comprised of vendors and users of process control automation. The PCSRF is applying the **ISO 15408 Common Criteria** methodology to develop Protection Profiles for process control.

Note: All information on this site is now password protected. Please visit the [Join the PCSRF](#) link to request a password if you have not done so.

<a href="#">Join the PCSRF</a>	<a href="#">What's New</a>
<a href="#">Upcoming Meetings</a>	<a href="#">Meeting Minutes and Reports</a>
<a href="#">Documents</a>	<a href="#">Resources and Links</a>
<a href="#">Participants</a>	<a href="#">Mailing List Information</a>

Document: Done (0.391 secs)



# System Protection Profile for Industrial Control Systems (SPP-ICS)

---

- 151 page generic system level protection profile for ICS
- Contains security functional and assurance requirements that extend ISO 15408 to address systems (ISO/IEC 19791)
- Presents a cohesive, cross-industry set of security requirements for new industrial process control systems
- Includes IT and non-IT security requirements
- Considers an entire system and addresses requirements for the entire system lifecycle
- A starting point for:
  - More specific system protection profiles (SCADA, DCS)
  - A System Security Target (SST) for a specific instance of an industrial control system
  - Component protection profiles (PPs) – e.g., industrial controller authentication, sensor authentication, etc.



# Main Recommendations

---

- Address security throughout the system life cycle
- Defense in depth approach
- Identification and authentication - users and data
- Event recording and auditing
- Reliable and standard (consistent) time stamps
- Encryption where required
- Secure out of the box
- Policies and procedures
  - Personnel
  - Configuration and patch management



# Security Requirements Packages Approach

---

Industry 1

Added  
Requirements

Specific  
Guidance

Industry 2  
additions

Industry 3  
additions

Component 1  
additions

Baseline System Protection Profile for Industrial Control Systems (SPP-ICS):

Common specification of requirements,  
application notes and guidance



# SCADA Protection Profile

---

- PCSR Working Group
  - 10 member group
  - Experienced in Common Criteria, SCADA systems and requirements
- Specific functional and assurance requirements for SCADA systems
- Comprised of 2 connected PPs
  - Control Center Protection Profile
  - Field Device and Communications Protection Profile



# SP800 SCADA/ICS Security Guideline

---

- Guidance for establishing secure SCADA and Industrial Control Systems
- Provides an overview and presents typical topologies to facilitate the understanding of industrial control systems
- Identifies typical vulnerabilities, threats and consequences
- Provides guidance on security deployment including administrative, physical and technical countermeasure to mitigate the associated risks
- Public draft by September 1, 2005 with final document completed by January 1, 2006



# Document Organization

---

- Executive Summary
- Introduction
- Industrial Control Systems
- Industrial Control Systems Vulnerabilities
- Industrial Control Systems Security Deployment
- Component/Vulnerabilities/Countermeasures Table
- Emerging Security Capabilities
- Case Study
- Appendices
  - Acronyms and Abbreviations
  - Glossary of Terms
  - Current Activities in SCADA/Industrial Control Security



# Audience

---

- Control engineers, integrators and architects when designing and implementing secure SCADA and/or industrial control systems
- System administrators, engineers and other IT professionals when administering, patching, securing SCADA and/or industrial control systems
- Security consultants when performing security assessments of SCADA and/or industrial control systems
- Managers responsible for SCADA and/or industrial control systems
- Researchers and analysts who are trying to understand the unique security needs of SCADA and/or industrial control systems
- Vendors developing products that will be deployed in SCADA and/or industrial control systems



# Industrial Control Systems

---

- Provides an overview of SCADA and industrial control systems
- Control Systems vs. Typical IT Systems
- SCADA Systems
- Industrial Process and Discrete Part Control Systems
- Control System Components and Connectivity



# Industrial Control Systems Vulnerabilities

---

- Discusses SCADA and industrial control systems vulnerabilities
- Administrative Vulnerabilities (policies and procedures)
- Physical Vulnerabilities
- Platform Vulnerabilities
- Network Vulnerabilities



# Industrial Control Systems Security Deployment

---

- Business case for security
- Layered security
- Recommended Management, Operational and Technical security controls (countermeasures) to mitigate the risk associated with the vulnerability



# Management Controls

---

- Risk Assessment
- Developing and Implementing a Security Program
- System and Services Acquisition
- Security Assessments



# Operational Controls

---

- Personnel Security
- Patch Management
- Configuration Management
- Checklists
- Network Segmentation
- Incident Response
- Disaster Recovery Planning
- Physical Protection



# Technical Controls

---

- User Identification, Authentication and Authorization
- Data Identification and Authentication
- Device Identification, Authentication and Authorization
- Logging
- Audit
- Secure Communications
- Access Control
- Intrusion Detection and Prevention
- Virus, Worm and Malicious Code Detection



# Component/Vulnerabilities/ Countermeasures Table

---

- Summarizes, in a tabular form
  - Components typically found in SCADA and industrial control systems
  - Vulnerabilities associated with each component
  - Recommended controls (countermeasures) to mitigate the risk associated with the vulnerability



# Emerging Security Capabilities

---

- Discusses emerging security capabilities that are being developed in the SCADA and industrial control system sector such as device authentication for field devices and encryption modules



# Case Study

---

- Discusses a case study in SCADA and industrial control system security



# Appendices

---

- Acronyms and Abbreviations
- Glossary of Terms
- Mapping of document control to SP800-53, ISO 17799, others?)
- Current Activities in SCADA/Industrial Control System Security
- References



# ICS Vendor Security Checklist Program

---

- Work with SCADA/ICS security and security-enabled product vendors/ manufactures to submit recommended security settings for their products to the current NIST IT Security Checklist Program
- Checklists are also commonly referred to as lockdown guides, hardening guides, security technical implementation guides (STIGS), or benchmark. A checklist could also contain scripts, templates, and pointers to patches, or updates or firmware upgrades that can be applied to the product.
- NIST Special Publication 800-70 *Security Configuration Checklists Program for IT Products* provides guidance for checklist developers and users



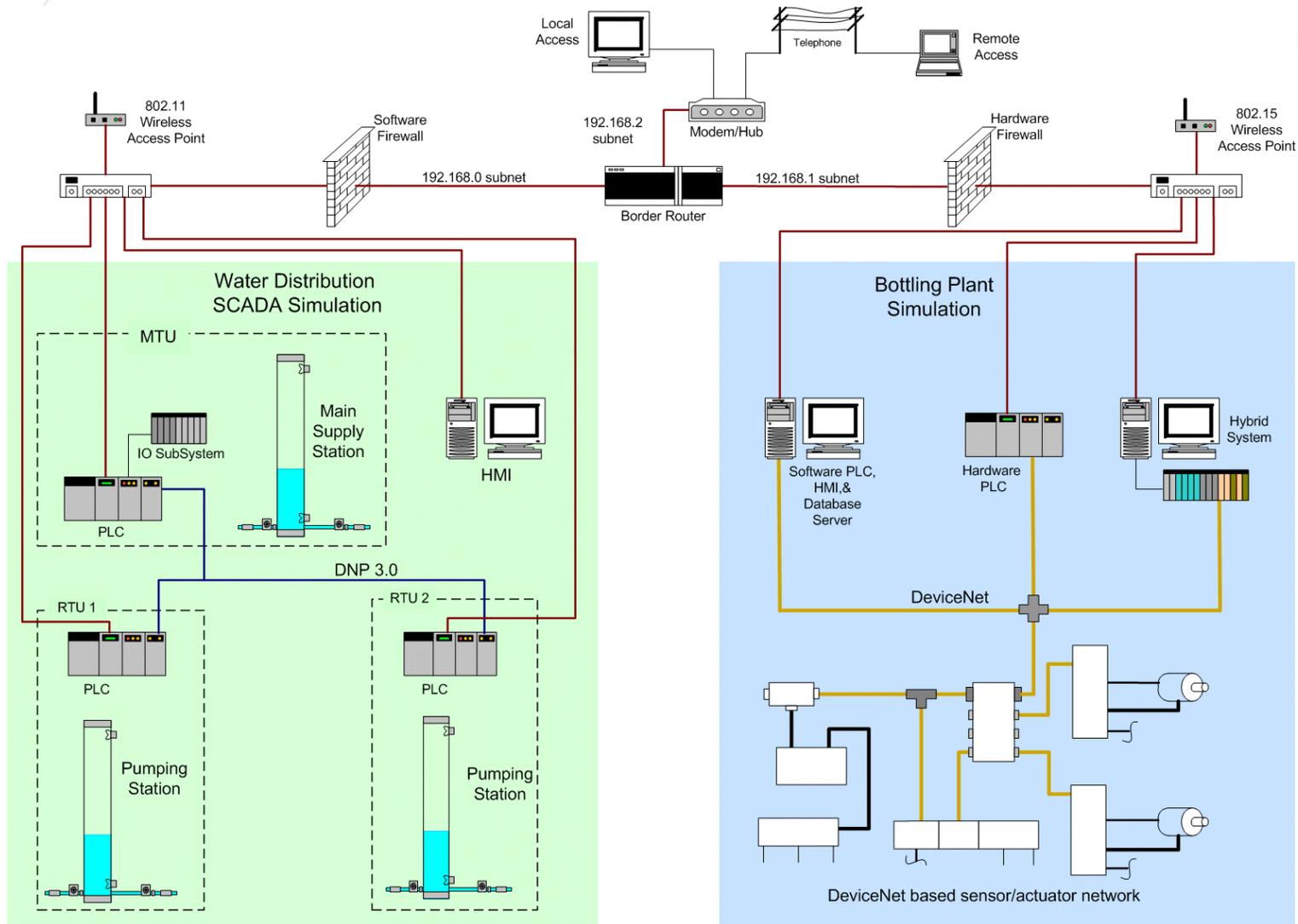
# NIST Industrial Control System Security Testbed

---

- Provides an industrial setting in which to
  - validate standards for process control security
  - develop performance- and conformance test methods
- Targeted outcomes:
  - development and dissemination of best practices for process control security
  - security standards for acquisition, development, and retrofit of industrial control systems



# NIST Industrial Control System Security Testbed Architecture





# Factory Control System

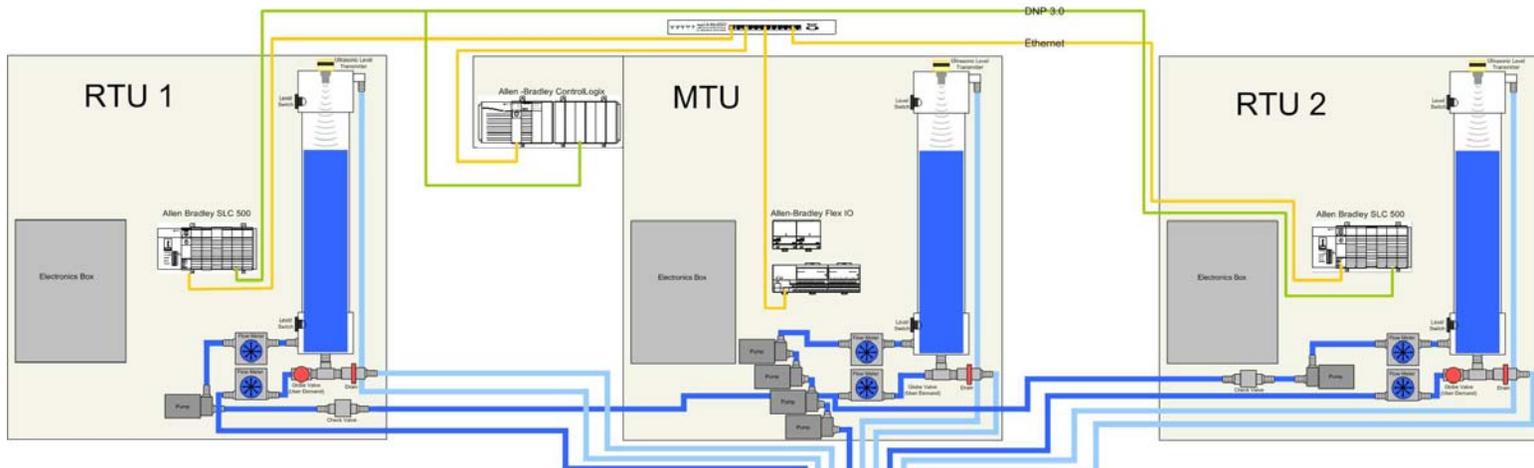
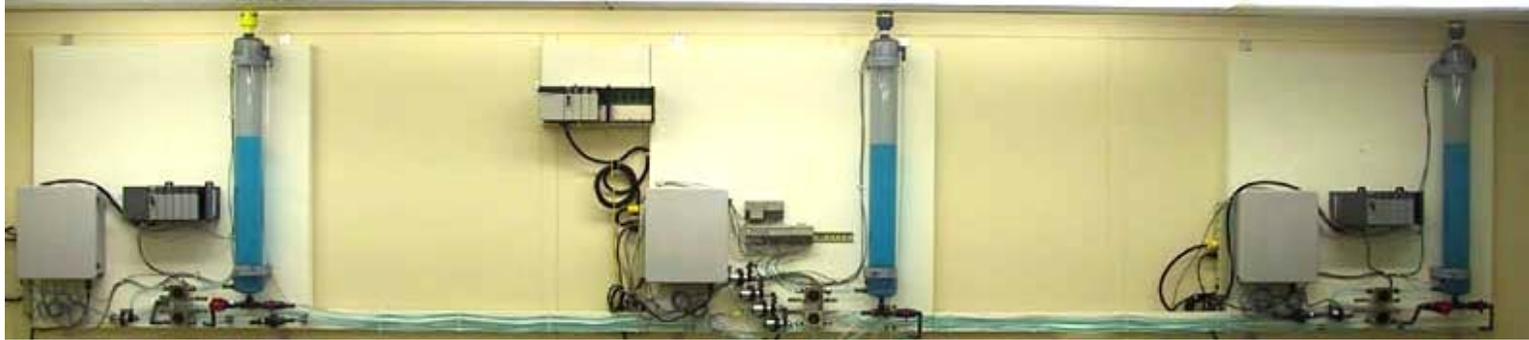


- DeviceNet I/O network
- Three controller options
  - Wonderware PC-based software PLC
  - Modicon hardware PLC
  - DeltaV Hybrid Controller
- SQL database for data logging



# Water Distribution SCADA System

- Ultrasonic Level Transmitters
- Analog Flow Meters
- DNP 3.0 Serial
- Liquid Level Switches
- Centrifugal Pumps
- Ethernet



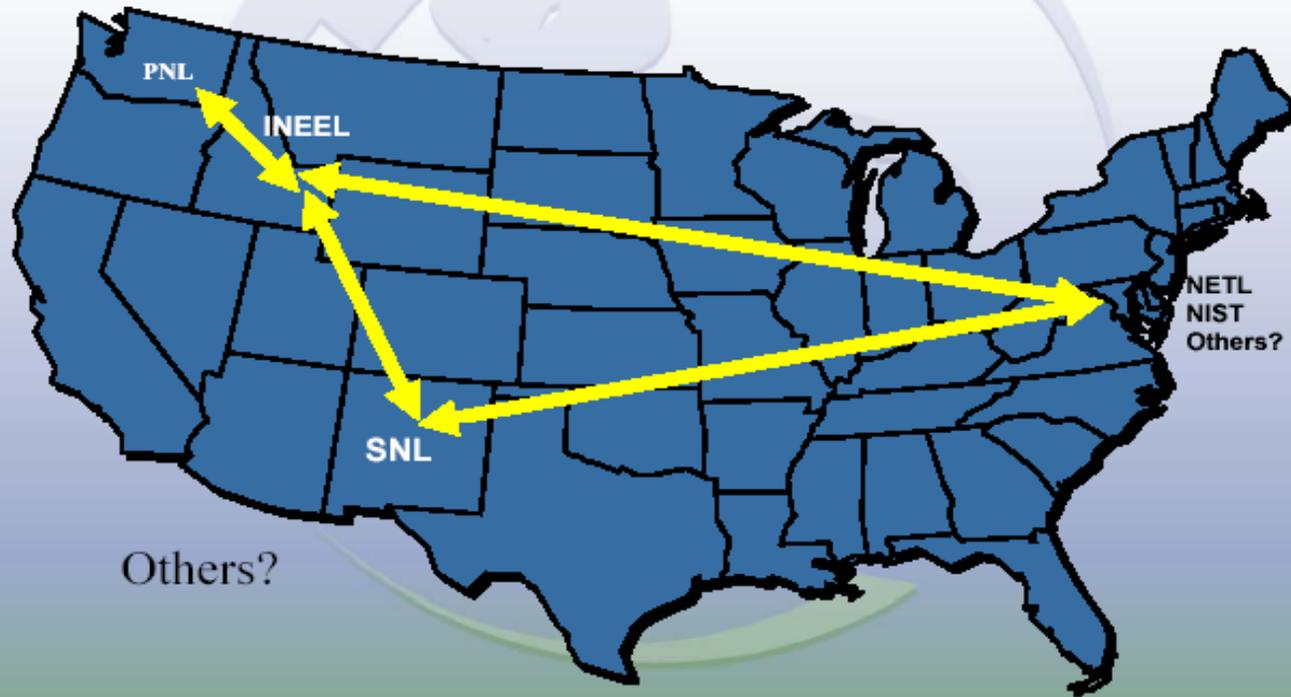


# National SCADA Testbed

Idaho National Engineering and Environmental Laboratory



***A Virtual, Distributed,  
SCADA Test Bed***





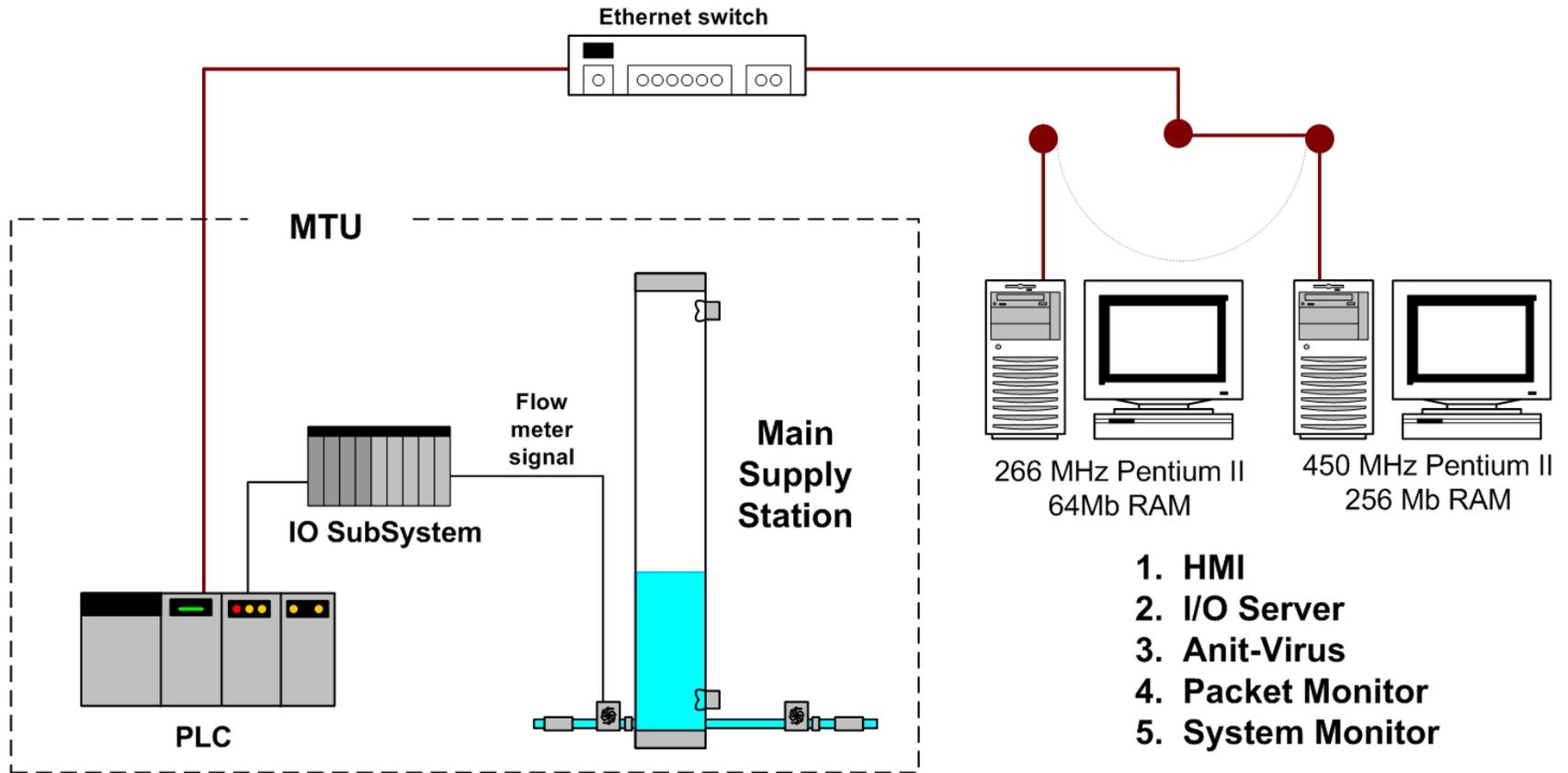
# Antivirus Test Methods

---

- Develop performance tests to screen for potential problems when deploying security software in industrial control system environments
- Test procedures, and guidance with accompanying data to illustrate potential problems and solutions when deploying security software with industrial control systems



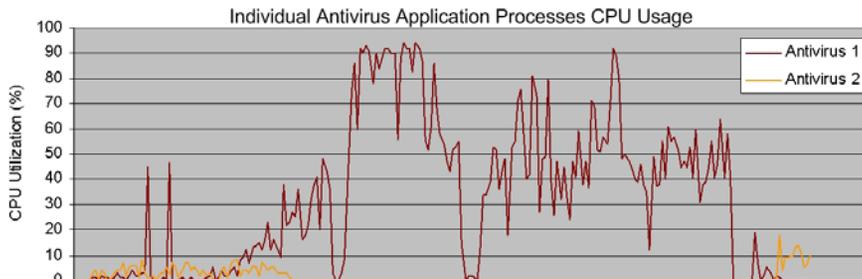
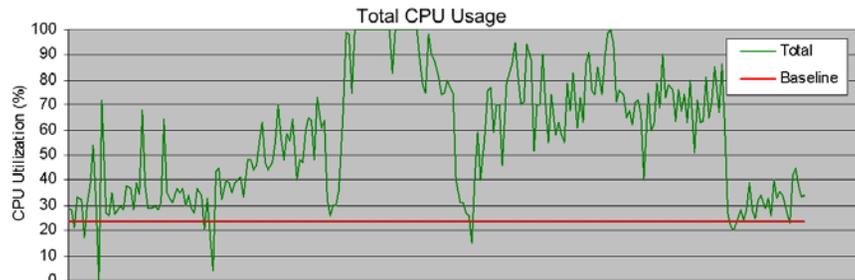
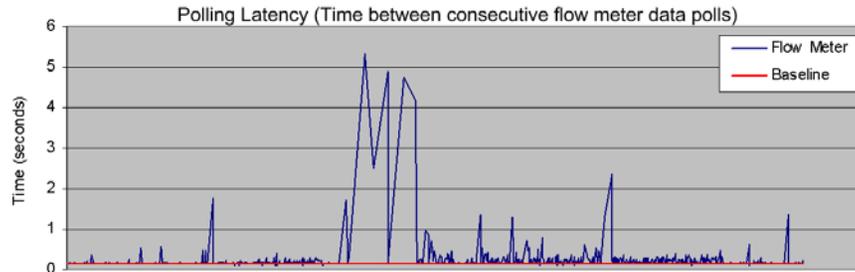
# Test Case





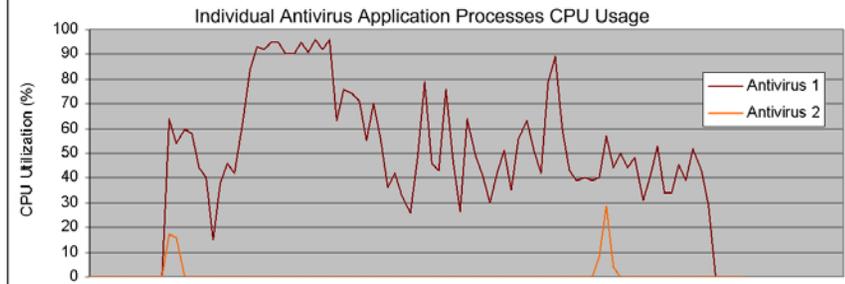
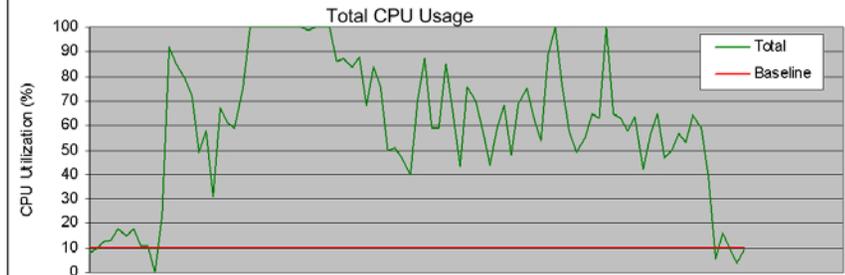
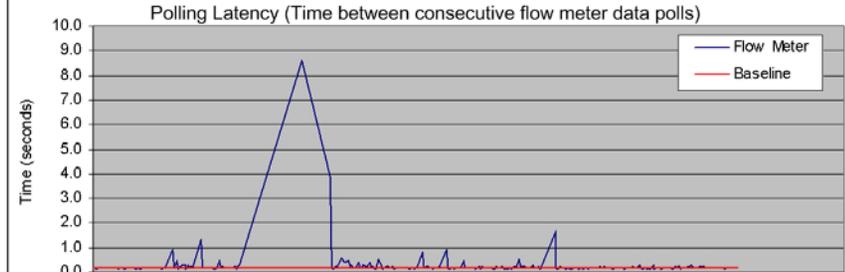
# Manual Scanning Hard Drive

Manual Scan (high priority) - Pentium II 266MHz/64Mb



Test Duration - 4.0 Minutes

Manual Scan (high priority) - Pentium II 450MHz/256Mb

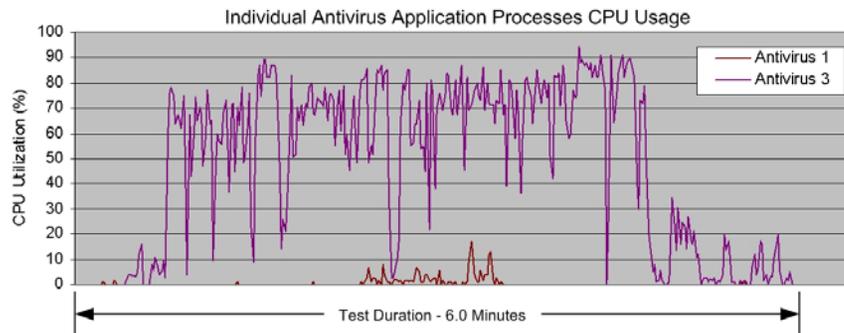
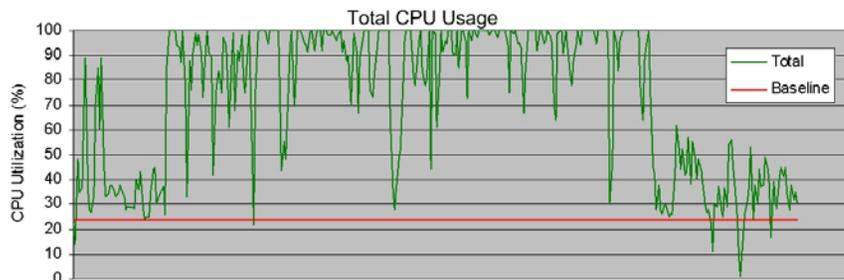
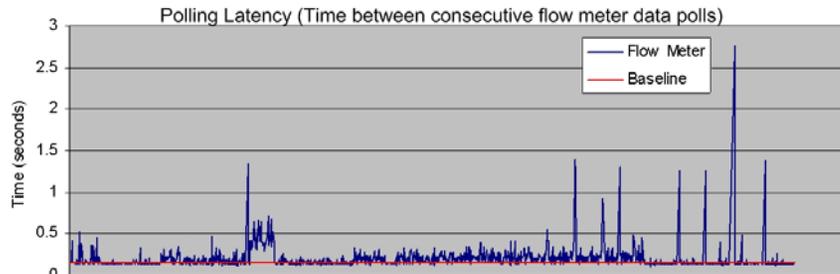


Test Duration - 1.5 Minutes

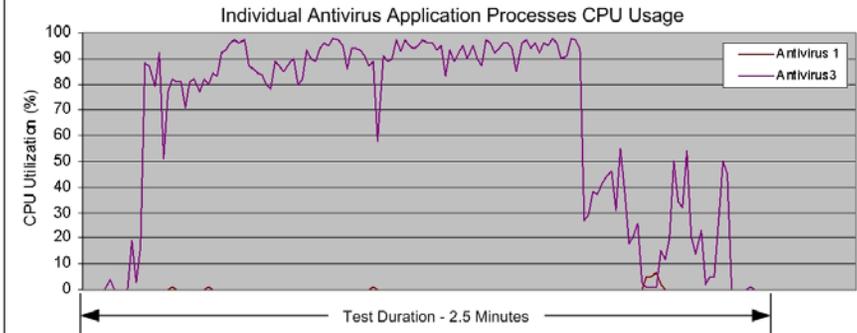
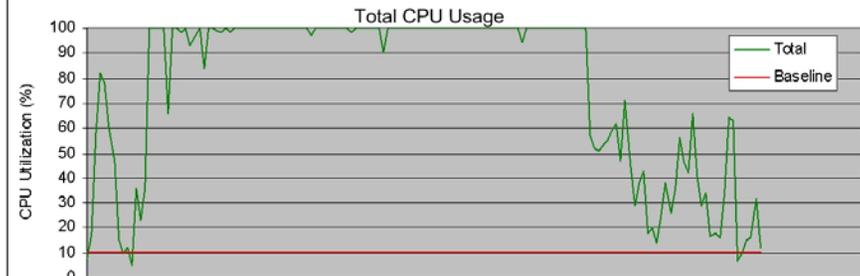
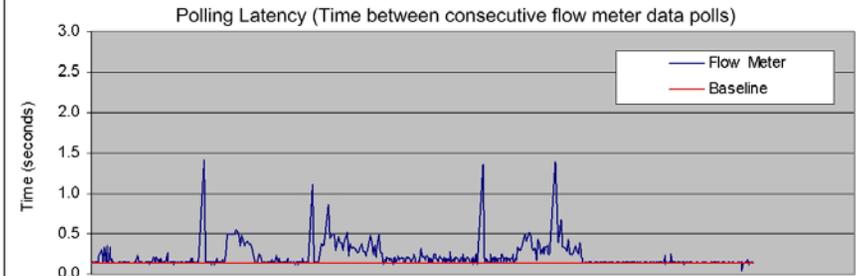


# Virus Definition Update

Virus Definitions Update - Pentium II 266MHz/64Mb



Virus Definitions Update - Pentium II 450MHz/256Mb





# Collaboration

---

- Cross laboratory collaboration with the Electronics and Electrical Engineering Laboratory (EEEL) and the Information Technology Laboratory (ITL) at NIST
- Standards body collaboration with ISA, including development of the ISA-SP99 standard and coordination with SP99 Chair on industrial control security activities
- Government collaboration with the Department of Homeland Security (DHS) including the Process Control Systems Forum (PCSF) and other government agencies including the Department of Energy (DOE)
- Testbed collaboration with the National SCADA Testbed (Idaho National Engineering and Environmental Laboratory and Sandia National Laboratory)



# The Instrumentation, Systems, and Automation Society (ISA)-SP99

---

- Developing an ANSI Standard for Industrial Control System Security
  - Part 1 – Models and Terminology
  - Part 2 – Establishing a Manufacturing and Control Systems Program –  
NIST is the technical editor for Part 2
  - Part 3 – Operating a Manufacturing and Control Systems Program
  - Part 4 – Specific Security Requirements for Manufacturing and Control Systems -  
Security requirements developed by PCSRF will feed Part 4 – due to start in 2006



# DHS Process Control Systems Forum (PCSF) [www.pcsforum.org](http://www.pcsforum.org)

**Process Control Systems Forum (PCSF) - Netscape 6**

File Edit View Search Go Bookmarks Tasks Help

https://www.pcsforum.org/

Home My Netscape Search Shop Bookmarks Net2Phone Brodia Wallet RealPlayer Ho...

**PROCESS CONTROL SYSTEMS FORUM**

Logged in as [keith.stouffer@nist.gov] HOME | FAQs | CONTACT US | FEEDBACK | MY ACCOUNT | LOGIN | SITE MAP

- About PCSF
- Governance Body
- News/PR
- Calendar of Events
- PCSF User Account
- Interest Groups
- Working Groups
- Knowledge Base
- Research Library

Google™

WWW  
www.pcsforum.org

Search

**Welcome to the Process Control Systems Forum (PCSF)**

The Department of Homeland Security has established a Process Control Systems Forum (PCSF). The PCSF is a unified effort between the National Cyber Security Division and Science & Technology to form a natural bridge between Government and Industry.

The purpose of the Process Control Systems Forum is to accelerate the development of technology that will enhance the security, safety and reliability of Process Control Systems (PCS) and Supervisory Control and Data Acquisition (SCADA) systems by providing a single venue for technologists from all user sectors, vendors, and academia to work together in evaluating, specifying, developing, refining and testing new technologies.

The PCSF is an open, collaborative, voluntary forum that will leverage the experience and capabilities of stakeholders in the development and adoption of common architectures, protocols, and practices for next generation control systems. Innovations developed by the forum will guide requirement gathering, testing, retro-fit, development, and deployment strategies. The PCSF will leverage knowledge currently dispersed among sectors, and stimulate cross-functional discussions between Information Technology (IT) and Operations to strengthen communication and resolve issues inherent within their respective disciplines.

The PCSF is not a standards body and is not intended to replace any existing activities in the PCS and SCADA community. The PCSF will build upon the existing body of work in this subject area, and establish links with others in industry and government to arrive at a common underlying architecture for process control systems that offers security, reliability, resiliency, and continuity in the face of disruptions and major incidents.

The PCSF will become a valuable organization through the active participation of individuals interested in advancing security and reliability in process control systems.

## PCSF Interim Governing Board Members

Position	Name
Forum Director	Robert Clerman Mitretek Systems, Inc.
Chair	Mike Lombard National Cyber Security Division Department of Homeland Security
Vice Chair	Bill Rush Gas Technology Institute
Member	Keith Stouffer National Institute of Science and Technology
Member	Tom Flowers CenterPoint Energy
Member	Kendra Martin American Petroleum Institute
Member	Hank Kenchington Department of Energy
Member	R. Russell Rhinehart School of Chemical Engineering, Oklahoma State University
Member	Mark Heard Eastman Chemicals
Member	Bryan Singer Vendor Community
Member	Seth Johnson Water and Waste Management Industry



# I3P SCADA Initiative

---

- Collaborating with Dartmouth since March 2005
- I3P SCADA Security Workshop June 2 and 3 in Houston
- Sent organizers approximately 40 contacts in the oil and gas industry (end users and vendors) for the June 2 and 3 workshop
- Met with I3P contacts at NIST, May 9 and during the May 17-19 PCSF/PCSRF meetings in Dallas



# SCADA Link Encryption

---

- NIST funded contract with Gas Technology Institute to develop performance tests for cryptographic protection modules in industrial control system environments
- Test procedures, and guidance with accompanying data to be used when deploying SCADA link encryption
- AGA 12 (SCADA Link Encryption Standard)



# GTI Testbed

- GTI Testbed to study the effects of cryptographic modules on the asynchronous communications networks used in SCADA systems





# Recent Outreach

---

- **Presentations/Publications**
  - Best Practices for Driving Operational Excellence in Manufacturing ARC Advisory Group Forum, Orlando, FL, January 2004.
  - I-4 Regional Meeting: Process Control Security, ExxonMobil Research and Engineering Co, Fairfax, VA, April 2004
  - 2004 TAPPI Paper Summit, Atlanta, May 2004
  - 2004 NDIA Homeland Security Symposium & Exhibition Hyatt Regency, Crystal City, Virginia, May 2004
  - Microsoft Executive Circle Manufacturing Security Summit, Redmond, WA, July 2004.
  - ISA Industrial Network Security Technical Conference “New Developments and Directions”, Philadelphia, PA, July 2004
  - Infosecurity 2004 New York, NY, December 2004
  - Water Environment Research Foundation Security Workshop, Washington DC, April 2005
  - 2<sup>nd</sup> International Symposium for Industrial Control Security, Vancouver, April 2005
  - PCSF/PCSRF Meetings, May 2005
- **Magazine articles**
  - Control Engineering, June 2004
  - Control, Federal Computer Week, October 2004
  - ComuputerWorld, InfoSec News, CSO Online, Computerweekly, Online Symantec Online, November 2004



# Summary

---

- Process control automation is heavily used in critical infrastructure
- Traditional IT security solutions can't blindly be applied to real-time, embedded devices and controllers
- Users, vendors and integrators are teaming to develop standards and products to address the needs
- NIST's role is working with industry to develop standards, guidelines, checklist and test methods for industrial control system security



# Additional Information

---

More information:

[www.isd.mel.nist.gov/projects/processcontrol](http://www.isd.mel.nist.gov/projects/processcontrol)

or

[www.niap.nist.gov](http://www.niap.nist.gov)

click *Forums* ⇒ *Process Control*